IN THE UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS
EASTERN DIVISION

ROBERT SMITH, on behalf of himself and others similarly situated, Plaintiff, v. **ZOLL MEDICAL CORPORATION,** Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Robert Smith individually and on behalf of all others similarly situated, brings this action against ZOLL Medical Corporation, ("ZOLL" or "Defendant"). The following allegations are based on Plaintiff's knowledge, investigations of counsel, facts of public record, and information and belief.

NATURE OF THE ACTION

1. Plaintiff seeks to hold Defendant responsible for the injuries ZOLL inflicted on Plaintiff and over 1 million others due to Defendant's impermissibly inadequate data security, which caused the personal and health information of Plaintiff and those similarly situated to be exposed to the public (the "Data Exposure").

2. ZOLL is Asahi Kasei company. It makes a variety of advanced emergency care devices that provide defibrillation and cardiac monitoring, circulation enhancement and CPR feedback, supersaturated oxygen therapy, ventilation, and more.

3. The data that Defendant exposed to the public is highly sensitive. According to Defendant's submission to the Maine Attorney General, the exposed data included personal identifying information ("PII") and protected health information ("PHI") like Social Security numbers, full names, dates of birth, and addresses. The exposed data also allowed individuals to infer that Plaintiff and Class Members were using or being considered for ZOLL products, disclosing their health conditions.[1]

4. Plaintiff received a Notice of Data Exposure Letter that did not specify the types of PII and PHI impacted; rather, his letter states that the Data Exposure "may have resulted in the disclosure of some of [his] protected health information."[2] Upon information and belief, the full scope of the PII and PHI impacted by the Data Exposure remains unknown.

5. According to the Notice of Data Exposure Letter Plaintiff received, On January 28, 2023, Defendant detected unusual activity on its internal network. Defendant determined that Plaintiff's and Class Members' PII and PHI was affected on or about February 2, 2023.

6. Upon information and belief, the risk of the Data Exposure was known to Defendant. Thus, Defendant was on notice that its inadequate data security created a heightened risk of exposure, compromise, and theft.

7. After the Data Exposure, Defendant failed to provide timely notice to Plaintiff and Class Members, thereby exacerbating their injuries. Ultimately, Defendant

[1] *See* Exhibit 1, Sample Notice of Data Exposure Letter Submitted to Maine Attorney General
[2] See Exhibit 2, Plaintiff's Notice of Data Exposure Letter

deprived Plaintiff and Class Members of the chance to take speedy measures to protect themselves and mitigate harm. Simply put, Defendant impermissibly left Plaintiff and Class Members in the dark—thereby causing their injuries to fester and the damage to spread.

8. Even when Defendant finally notified Plaintiff and Class Members of the disclosure[3], Defendant failed to adequately describe what information was compromised.

9. Today, the identities of Plaintiff and Class Members are in jeopardy because of Defendant's negligence. Plaintiff and Class Members now suffer from a heightened and imminent risk of fraud and identity theft and must now constantly monitor their financial accounts.

10. The PII and PHI exposed in the Data Exposure can enable criminals to commit a litany of crimes. Criminals can now open new financial accounts in Class Members' names, take out loans using Class Members' identities, use Class Members' names to obtain medical services, use Class Members' health information to craft phishing and other hacking attacks based on Class Members' individual health needs, use Class Members' identities to obtain government benefits, file fraudulent tax returns using Class Members' information, obtain driver's licenses in Class Members' names (but with another person's photograph), and give false information to police during an arrest.

[3] *See id.*

11. Plaintiff and Class Members will likely suffer additional financial costs for purchasing necessary credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect fraud and identity theft.

12. Plaintiff and Class Members have suffered—and will continue to suffer—from the loss of the benefit of their bargain, unexpected out-of-pocket expenses, lost or diminished value of their PII and PHI, emotional distress, and the value of their time reasonably incurred to mitigate the fallout of the Defendant's Data Exposure.

13. Through this action, Plaintiff seeks to remedy these injuries on behalf of themselves and all similarly situated individuals whose PII and PHI were exposed and compromised in the Data Exposure.

14. Plaintiff seeks remedies including, but not limited to, compensatory damages, treble damages, punitive damages, reimbursement of out-of-pocket costs, and injunctive relief—including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

15. Plaintiff brings this action against Defendant and asserts claims for: (1) negligence, (2) negligence per se, (3) unjust enrichment, and (4) breach of fiduciary duty.

PARTIES

16. Plaintiff Robert Smith is a natural person, resident, and citizen of Virginia.

17. Defendant ZOLL Medical Corporation is a Massachusetts entity with a principal place of business and headquarters at 269 Mill Road, Chelmsford, Massachusetts.

JURISDICTION AND VENUE

18. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. And minimal diversity is established because Plaintiff (and many members of the class) are citizens of states different than Defendant.

19. This Court has general personal jurisdiction over Defendant because Defendant's principal place of business and headquarters is in Chelmsford, Massachusetts. Defendant also regularly conduct substantial business in Massachusetts.

20. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) because substantial part of the events giving rise to the claims emanated from activities within this District, and Defendant conduct substantial business in this District.

FACTUAL ALLEGATIONS

Defendant Collected and Stored the PII and PHI of Plaintiff and Class Members

21. ZOLL is an Asahi Kasei company that makes a variety of advanced emergency care devices that provide defibrillation and cardiac monitoring, circulation enhancement and CPR feedback, supersaturated oxygen therapy, ventilation, and more. ZOLL "provide[s] innovative technologies that make a meaningful difference in people's

lives. [Its] medical devices, software, and related services are used worldwide to diagnose and treat patients suffering from serious cardiopulmonary and respiratory condition."[4]

22. ZOLL states that, "[w]ith products for defibrillation and cardiac monitoring, circulation enhancement and CPR feedback, supersaturated oxygen therapy, data management, ventilation, therapeutic temperature management, and sleep apnea diagnosis and treatment, ZOLL provides a comprehensive set of technologies that help clinicians, EMS and fire professionals, as well as lay rescuers, improve patient outcomes in critical cardiopulmonary conditions."[5]

23. Plaintiff's and Class Member's PII and PHI was provided to Defendant in conjunction with the type of work Defendant does within the healthcare industry.

24. Upon information and belief, Defendant collects and maintains PII and PHI such as customers' full names, Social Security Numbers, address, date of birth, as well as medical information in the ordinary course of business. These records are stored on Defendant's computer systems.

25. Because of the highly sensitive and personal nature of the information Defendant acquires and stores, Defendant knew or reasonably should have known that it stored protected PII and PHI and therefore must comply with healthcare industry standards related to data security and all federal and state laws protecting customers' and patients' PII and PHI and provide adequate notice to customers if their PII or PHI is disclosed without proper authorization.

---

[4] https://www.zoll.com/about-zoll/company-overview (last accessed Mar. 13, 2023).
[5] *See id*.

26. Upon information and belief, when Defendant collects this sensitive information, it promises to use reasonable measures to safeguard the PII and PHI from theft and misuse.

27. Defendant acquired, collected, and stored sensitive information, while representing that it maintained reasonable security over that information.

28. By obtaining, collecting, receiving, and/or storing Plaintiff's and Class Members' PII and PHI, Defendant assumed legal and equitable duties and knew, or should have known, that it was responsible for protecting Plaintiff's and Class Members' PII and PHI from unauthorized disclosure.

29. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI, including but not limited to, protecting their usernames and passwords, using only strong passwords for their accounts, and refraining from browsing potentially unsafe websites.

30. Upon information and belief, Plaintiff and Class Members relied on Defendant to keep their PII and PHI confidential and securely maintained, to use this information for business and healthcare purposes only, and to make only authorized disclosures of this information.

31. Defendant could have prevented the Data Exposure by properly securing and encrypting and/or more securely encrypting its servers generally, as well as Plaintiff's and Class Members' PII and PHI.

32. Defendant's negligence in safeguarding Plaintiff's and Class Members' PII and PHI was exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years.

33. The healthcare industry in particular has experienced a large number of high-profile cyberattacks even in just the short period preceding the filing of this Complaint, and cyberattacks, generally, have become increasingly more common. More healthcare data breaches were reported in 2020 than in any other year, showing a 25% increase.[6] Additionally, according to the HIPAA Journal, the largest healthcare data breaches have been reported beginning in April 2021.[7]

34. In the context of data breaches, healthcare is "by far the most affected industry sector."[8] Further, cybersecurity breaches in the healthcare industry are particularly devastating, given the frequency of such breaches and the fact that healthcare providers maintain highly sensitive and detailed PII.[9] And according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[10]

---

[6] *2020 Healthcare Data Exposure Report,* HIPAA JOURNAL (Jan. 19, 2021) https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/.

[7] *April 2021 Healthcare Data Exposure Report,* HIPAA JOURNAL (May 18, 2021) https://www.hipaajournal.com/april-2021-healthcare-data-breach-report/.

[8] Tenable Security Response Team, *Healthcare Security*, TENABLE (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches.

[9] *See id.*

[10] *See* Maria Henriquez, *Iowa City Hospital Suffers Phishing Attack*, SECURITY MAGAZINE (Nov. 23, 2020), https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack.

35. Despite the prevalence of public announcements of data breaches and data security compromises, Defendant failed to take appropriate steps to protect Plaintiff's and Class Members' PII and PHI from being compromised.

36. Defendant failed to properly train its employees as to cybersecurity best practices and to maintain proper staffing and processes for responding to and preventing network intrusions.

37. Upon information and belief, Defendant failed to implement sufficient processes to quickly detect and respond to data breaches, security incidents, or intrusions.

38. Upon information and belief, Defendant failed to encrypt Plaintiff's and Class Members' PII and PHI and monitor user behavior and activity to identify possible threats.

39. Defendant failed to provide fair, reasonable, or adequate computer systems and data security practices to safeguard the PII and PHI of Plaintiff and Class Members.

40. Defendant failed to timely and accurately disclose that Plaintiff's and Class Members' PII and PHI had been improperly acquired or accessed.

41. Defendant knowingly disregarded standard information security principles, despite obvious risks, by allowing unmonitored and unrestricted access to unsecured PII and PHI.

The Data Exposure

42. ZOLL's Notice of Data Exposure Letter Submitted to the Maine Attorney General states that:

> On January 28, 2023, we detected unusual activity on our internal network, and we promptly took steps to mitigate the incident. We consulted with third-party cybersecurity experts to assist with our response to the incident, and we notified law enforcement. We determined that your information may have been affected on or about February 2, 2023. Our investigation into the incident is ongoing.[11]

43. The letter further states that:

> Information that may have been disclosed includes your name, address, date of birth, and Social Security number. It may also be inferred that you used or were considered for use of a ZOLL product.[12]

44. The letter otherwise gives no details to Class Members regarding the manner and means of how their information was disclosed and leaves Class Members wondering how they can protect themselves.

45. Upon information and belief, Plaintiff's and Class Members' PII and PHI was disclosed during the Data Exposure.

46. Upon information and belief, Plaintiff's and Class Members' affected PII and PHI was accessible, unencrypted, unprotected, and vulnerable for acquisition and/or exfiltration by unauthorized individuals.

47. It is likely the Data Exposure was discovered by cybercriminals due to Defendant's status as healthcare related entity that collects, creates, and maintains both PII and PHI.

48. Time is of the essence when highly sensitive PII and PHI is subject to unauthorized access and/or acquisition. The disclosed, accessed, and/or acquired PII and

---

[11] See Exhibit 1, Notice of Data Exposure Letter Submitted to Maine Attorney General
[12] See *id.*

PHI of Plaintiff and Class Members is likely available on the Dark Web. Hackers can access and then offer for sale the unencrypted, unredacted PII and PHI to criminals.

49. Plaintiff and Class Members are now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from the possible publication of their PII and PHI, especially their Social Security numbers and sensitive medical information, onto the Dark Web. Plaintiff and Class Members now face a lifetime risk of identity theft, which is heightened here by unauthorized access, disclosure, and/or activity by cybercriminals on computer systems containing hundreds of thousands of Social Security numbers and/or specific, sensitive medical information.

50. Defendant largely put the burden on Plaintiff and Class Members to take measures to protect themselves from identity theft and fraud.

51. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.[13]

52. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per

[13] *Characteristics of minimum wage workers, 2020*, U.S. BUREAU OF LABOR STATISTICS https://www.bls.gov/opub/reports/minimum-wage/2020/home.htm#:~:text=In%202020%2C%2073.3%20million%20workers,wage%20of%20%247.25%20per%20hour (last accessed Jan. 30, 2023); *Average Weekly Wage Data*, U.S. BUREAU OF LABOR STATISTICS, *Average Weekly Wage Data,* https://data.bls.gov/cew/apps/table_maker/v4/.table_maker.htm%23type=1&year=2021&qtr=3&own=5&ind=10&supp=0 (last accessed Aug. 2, 2022) (finding that on average, private-sector workers make $1,253 per 40-hour work week.).

week;[14] leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"[15] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Exposure, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

53. Plaintiff and Class Members are now deprived of the choice as to how to spend their valuable free hours and seek renumeration for the loss of valuable time as another element of damages.

54. Defendant offered identity monitoring services for a period of 24 months. Such measures, however, are insufficient to protect Plaintiff and Class Members from the lifetime risks they each now face. As another element of damages, Plaintiff and Class Members seek a sum of money sufficient to provide to Plaintiff and Class Members identity theft protection services for their respective lifetimes.

55. Defendant's Notice of Data Exposure Letter omits the size and scope of the breach. Defendant has demonstrated a pattern of providing inadequate notices and disclosures about the Data Exposure.

---

[14] Cory Stieg, *You're spending your free time wrong — here's what to do to be happier and more successful*, CNBC https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html (Nov. 6, 2019).

[15] *Id.*

56. Plaintiff and the Class Members remain, even today, completely in the dark regarding what particular data was stolen, the particular method of disclosure, the results of any investigations, and what steps are being taken, if any, to secure their PII and PHI going forward. Plaintiff and Class Members are left to speculate as to the full impact of the Data Exposure and how exactly Defendant intends to enhance its information security systems and monitoring capabilities so as to prevent further breaches.

Defendant Failed to Comply with FTC Guidelines

57. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making.[16] To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII and PHI.

58. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[17] The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

[16] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (June 2015), https://bit.ly/3uSoYWF (last accessed Jan. 30, 2023).
[17] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Oct. 2016), https://bit.ly/3u9mzre (last accessed Jan.30, 2023).

59. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

60. The FTC recommends that companies not maintain PII and PHI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[18]

61. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

62. These FTC enforcement actions include actions against healthcare providers and partners like Defendant. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

[18] *See Start with Security*, *supra* note 46.

63. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Failed to Follow Industry Standards

64. Despite its alleged commitments to securing sensitive patient data, Defendant does not follow industry standard practices in securing patients' PII and PHI.

65. As shown above, experts studying cyber security routinely identify healthcare related entities as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

66. Several best practices have been identified that at a minimum should be implemented by healthcare providers like Defendant, including but not limited to, educating all employees on the risks of cyberattacks; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

67. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

68. Defendant failed to meet the minimum standards of any of the following

frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

69. Such frameworks are the existing and applicable industry standards in the healthcare industry. And Defendant failed to comply with these accepted standards, thus opening the door to criminals and the Data Exposure.

Defendant Violated HIPAA

70. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[19]

71. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII and PHI is properly maintained.[20]

---

[19] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[20] *See* 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308 (administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. § 164.312 (technical safeguards).

72. The Data Exposure itself resulted from a combination of inadequacies showing Defendant failed to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

a. Failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPAA security standards by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain and correct security violations in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

73. Defendant recognizes that it is a Business Associate under HIPAA and agrees that it will comply with HIPAA.[21] Simply put, however, the Data Exposure resulted from a combination of insufficiencies that demonstrate Defendant indeed failed to comply with safeguards mandated by HIPAA regulations.

The Experiences and Injuries of Plaintiff

74. Plaintiff and Class Members are the current and former patients of ZOLL. And as a prerequisite of receiving medical devices or treatment from ZOLL, Defendant required Plaintiff and Class Members to disclose their PII and PHI.

[21] *See* https://www.zolldata.com/business-associate-addendum

75. Defendant began notifying victims about the Data Exposure on or around March 13, 2023—over a month after discovering the Data Exposure.

76. When Defendant finally announced the Data Exposure, it deliberately underplayed the Exposure's severity and obfuscated the nature of the Exposure. Defendant's Exposure Notice sent to patients fails to adequately explain how the breach occurred, what exact data elements of each affected individual were compromised, and the extent to which those data elements were compromised.

77. Because of the Data Exposure, Defendant inflicted injuries upon Plaintiff and Class Members. And yet, Defendant has done little to provide Plaintiff and the Class Members with relief for the damages they suffered.

78. Plaintiff entrusted his PII and PHI to Defendant in conjunction with receiving treatment for cardiac issues in approximately 2020. Plaintiff had the reasonable expectation and understanding that Defendant would take—*at minimum*—industry standard precautions to protect, maintain, and safeguard that information from unauthorized users or disclosure, and would timely notify him of any data security incidents. After all, Plaintiff would not have entrusted their PII and PHI to Defendant had he known that Defendant would not take reasonable steps to safeguard his information.

79. Plaintiff suffered actual injury from having his PII and PHI compromised in the Data Exposure including, but not limited to, (a) damage to and diminution in the value of their PII and PHI—a form of property that Defendant obtained from Plaintiff; (b) violation of his privacy rights; (c) the likely theft of his PII and PHI; (d) fraudulent activity

resulting from the Exposure; and (e) present and continuing injury arising from the increased risk of additional identity theft and fraud.

80. As a result of the Data Exposure, Plaintiff also suffered emotional distress because of the release of his PII and PHI—which he believed would be protected from unauthorized access and disclosure.

81. Because of the Data Exposure, Plaintiff has spent—and will continue to spend—considerable time and money to try to mitigate and address harms caused by the Data Exposure.

82. On March 13, 2023, after Plaintiff received the Notice of Data Exposure Letter from Defendant, Plaintiff checked his bank account and found an unauthorized charge for $49.99. Plaintiff spent significant time resolving this unauthorized charge, which he believes was a result of the Data Exposure.

83. As a result of the Data Exposure and Defendant's Notice of Data Exposure Letter, Plaintiff made reasonable efforts to mitigate the impact of the Data Exposure, including but not limited to researching the Data Exposure checking his accounts for fraud and freezing his credit accounts.

84. Plaintiff has spent approximately over twelve hours responding to the Data Exposure and will continue to spend valuable time he otherwise would have spent on other activities, including but not limited to work and/or recreation.

85. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Exposure and has experienced anxiety and increased concerns for the

loss of his privacy, as well as anxiety over the impact of cybercriminals accessing and using his PII and PHI.

86. Plaintiff has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff and the Class Face Significant Risk of Present and Continuing Identity Theft

87. Plaintiff and Class Members suffered injury from the misuse of their PII and PHI that can be directly traced to Defendant.

88. The ramifications of Defendant's failure to keep Plaintiff's and the Class's PII and PHI secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

89. According to experts, one out of four data breach notification recipients become a victim of identity fraud.[22]

90. As a result of Defendant's failures to prevent—and to timely detect—the Data Exposure, Plaintiff and Class Members suffered and will continue to suffer damages,

[22] *More Than 12 Million Identity Fraud Victims in 2012 According to Latest Javelin Strategy & Research Report*, BUSINESSWIRE (Feb. 20, 2013) https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/.

including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII and PHI is used;

b. The diminution in value of their PII and PHI;

c. The compromise and continuing publication of their PII and PHI;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Exposure, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII and PHI; and

h. The continued risk to their PII and PHI, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII and PHI in their possession.

91. Stolen PII and PHI is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII and PHI can be worth up to $1,000.00 depending on the type of information obtained.[23]

92. The value of Plaintiff's and the Class's PII and PHI on the black market is considerable. Stolen PII and PHI trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

93. It can take victims years to spot or identify PII and PHI theft, giving criminals plenty of time to milk that information for cash.

94. One such example of criminals using PII and PHI for profit is the development of "Fullz" packages.[24]

95. Cyber-criminals can cross-reference two sources of PII and PHI to marry unregulated data available elsewhere to criminally stolen data with an astonishingly

---

[23] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017) https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

[24] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz", which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SECURITY, (Sep. 18, 2014) https://krebsonsecurity.com/tag/fullz/.

complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

96. The development of "Fullz" packages means that stolen PII and PHI from the Data Exposure can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII and PHI stolen by the cyber-criminals in the Data Exposure, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and other members of the proposed Class's stolen PII and PHI is being misused, and that such misuse is fairly traceable to the Data Exposure.

97. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.

98. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendant did not rapidly report to Plaintiff and the Class that their PII and PHI had been stolen.

99. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

100. In addition to out-of-pocket expenses that can exceed thousands of dollars and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by the theft of their PII and PHI. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

101. The Federal Trade Commission ("FTC") has also recognized that consumer data is a new and valuable form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[25]

102. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making.[26] According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment

---

[25] *Commissioner Pamela Jones Harbour: Remarks Before FTC Exploring Privacy Roundtable*, FED. TRADE COMMISSION (Dec. 7, 2009), https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-ftc-exploring-privacy-roundtable/091207privacyroundtable.pdf.

[26] *Start With Security, A Guide for Business*, FED. TRADE COMMISSION, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Oct. 21, 2022).

card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.[27]

103. According to the FTC, unauthorized PII and PHI disclosures are extremely damaging to consumers' finances, credit history and reputation, and can take time, money, and patience to resolve the fallout.[28] The FTC treats the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5(a) of the FTC Act (the "FTCA").

104. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Services, Inc.*, No. C-4326, ¶ 7 (June 15, 2011) ("[Defendant] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ¶ 7 (Mar. 7, 2006) ("[Defendant] failed to employ sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008)

---

[27] *Id.*

[28] *See Taking Charge, What to Do If Your Identity is Stolen*, FED. TRADE COMMISSION, at 3 (2012), https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen.

("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Defendant] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . ."). These orders, which all preceded the Data Exposure, further clarify the measures businesses must take to meet their data security obligations. Defendant thus knew or should have known that its data security protocols were inadequate and were likely to result in the unauthorized access to and/or theft of PII and PHI.

105. The healthcare industry has "emerged as a primary target [for data breaches] because [it sits] on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies to next of kin and credit cards, no other organization, including credit bureaus, ha[s] so much monetizable information stored in their data centers."[29]

106. Charged with handling highly sensitive PII and PHI including healthcare information, financial information, and insurance information, Defendant knew or should have known the importance of safeguarding the PII and PHI that was entrusted to it.

[29] Eyal Benishti, *How to Safeguard Hospital Data from Email Spoofing Attacks*, INSIDE DIGITAL HEALTH (Apr. 4, 2019), https://bit.ly/3x6fz08.

Defendant also knew or should have known of the foreseeable consequences if its data security systems were breached. This includes the significant costs that would be imposed on Defendant's customers' patients as a result of a breach. Defendant nevertheless failed to take adequate cybersecurity measures to prevent the Data Exposure from occurring.

107. Defendant's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has exposed the PII and PHI of Plaintiff and over 1 million members of the proposed Class to unscrupulous operators, con artists, and outright criminals.

CLASS ACTION ALLEGATIONS

108. Plaintiff brings this action on behalf of himself and on behalf of all other persons similarly situated ("the Class") under Fed. R. Civ. P. 23(b)(2), 23(b)(3), and 23(c)(4).

109. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All persons residing in the United States whose PII or PHI was impacted by the Data Exposure—including all persons that Defendant sent a notice of the Data Exposure to (the "Class").

110. The Class defined above is readily ascertainable from information in Defendant's possession. Thus, such identification of Class Members will be reliable and administratively feasible.

111. Excluded from the Class are: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Defendant or their parent has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; (6) members of the jury; and (7) the legal representatives, successors, and assigns of any such excluded persons.

112. Plaintiff reserves the right to amend or modify the Class definition as this case progresses.

113. Plaintiff satisfies the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23.

114. **Numerosity**. Class Members are numerous such that joinder is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of the approximately one million individuals whose PII and PHI were compromised by Defendant's Data Exposure.

115. **Commonality**. There are many questions of law and fact common to the Class. And these common questions predominate over any individualized questions of individual Class Members. These common questions of law and fact include, without limitation:

a. If Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII and PHI;

b. If Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Exposure;

c. If Defendant's data security systems prior to and during the Data Exposure complied with applicable data security laws and regulations including, *e.g.*, HIPAA;

d. If Defendant's data security systems prior to and during the Data Exposure were consistent with industry standards;

e. If Defendant owed a duty to Class Members to safeguard their PII and PHI;

f. If Defendant breached its duty to Class Members to safeguard their PII and PHI;

g. If Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. If Defendant should have discovered the Data Exposure earlier;

i. If Defendant took reasonable measures to determine the extent of the Data Exposure after it was discovered;

j. If Defendant's delay in informing Plaintiff and Class Members of the Data Exposure was unreasonable;

k. If Defendant's method of informing Plaintiff and Class Members of the Data Exposure was unreasonable;

l. If Defendant's conduct was negligent;

m. If Plaintiff and Class Members were injured as a proximate cause or result of the Data Exposure;

n. If Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

o. If Defendant breached implied contracts with Plaintiff and Class Members;

p. If Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

q. If Defendant failed to provide notice of the Data Exposure in a timely manner, and;

r. If Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

116. **Typicality**. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Exposure. Moreover, Plaintiff and Class Members were subjected to Defendant's uniformly illegal and impermissible conduct.

117. **Adequacy of Representation**. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's counsel are competent and

experienced in litigating complex class actions. Plaintiff has no interests that conflict with, or are antagonistic to, those of the Class.

118. **Predominance**. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that Plaintiff's and Class Members' data was stored on the same computer system and unlawfully exposed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

119. **Superiority**. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources, the parties' resources, and protects the rights of each Class Member.

120. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

121. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

122. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include those set forth above.

123. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

124. Plaintiff re-alleges and incorporates by reference paragraphs 1-122 of the Complaint as if fully set forth herein.

125. Defendant required its customers and patients to submit PII and PHI to receive Defendant's services.

126. By collecting and storing this data in their computer system and network, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard their computer system—and Plaintiff's and Class Members' PII and PHI held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes so they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

127. The risk that unauthorized persons would attempt to gain access to the PII and PHI and misuse it was foreseeable. Given that Defendant hold vast amounts of PII and PHI, it was inevitable that unauthorized individuals would at some point try to access Defendant's databases of PII and PHI.

128. After all, PII and PHI is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII and PHI of Plaintiff and Class Members. Thus, Defendant knew, or should have known, the importance of exercising reasonable care in handling the PII and PHI entrusted to them.

129. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the PII and PHI.

130. Defendant's duty of care to use reasonable security measures arose because of the special relationship that existed between Defendant and patients, which is recognized by laws and regulations including but not limited to HIPAA, as well as common law. Defendant was in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

131. Defendant failed to take appropriate measures to protect the PII and PHI of Plaintiff and the Class. Defendant is morally culpable, given the prominence of security breaches in the healthcare industry. Any purported safeguards that Defendant had in place were wholly inadequate.

132. Defendant breached its duty to exercise reasonable care in safeguarding and protecting Plaintiff's and the Class members' PII and PHI by failing to adopt, implement, and maintain adequate security measures to safeguard that information, despite known data breaches in the healthcare industry, and allowing unauthorized access to Plaintiff's and the other Class Members' PII and PHI.

133. The failure of Defendant to comply with industry and federal regulations evinces Defendant's negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII and PHI.

134. But for Defendant's wrongful and negligent breach of their duties to Plaintiff and the Class, patients' PII and PHI would not have been compromised, stolen, and viewed by unauthorized persons. Defendant's negligence was a direct and legal cause of the theft of the PII and PHI of Plaintiff and the Class and all resulting damages.

135. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other Class members' PII and PHI. Defendant knew or should have known that their systems and technologies for processing and securing the PII and PHI of Plaintiff and the Class had security vulnerabilities.

136. As a result of this misconduct by Defendant, the PII, PHI, and other sensitive information of Plaintiff and the Classes was compromised, placing them at a greater risk of identity theft and their PII and PHI being disclosed to third parties without the consent of Plaintiff and the Class.

SECOND CAUSE OF ACTION

Negligent Per Se
(On Behalf of Plaintiff and the Class)

137. Plaintiff re-alleges and incorporates by reference paragraphs 1-135 of the Complaint as if fully set forth herein.

138. Defendant had a duty to protect and maintain and provide adequate data security to maintain Plaintiff and the Class's PII and PHI under § 5 of the FTC Act, 15 U.S.C. § 45.

139. The FTC Act prohibits unfair business practices affecting commerce, which the FTC has interpreted to include a failure to use reasonable measures to safeguard Sensitive Information.

140. Defendants' violation of these duties is negligence per se under Massachusetts law.

141. Plaintiff and the proposed Class are included in the class of persons that the FTC Act was intended to protect.

142. The harm the Data Exposure caused is the type the FTC Act was intended to guard against.

143. Defendant's negligence per se caused Plaintiff and the proposed Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their Sensitive Information by criminals, improper disclosure of their Sensitive Information, lost benefit of their bargain, lost value of their Sensitive Information, and lost time and money incurred to mitigate and remediate the effects of the Data Exposure that resulted from and

were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which

THIRD CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

144. Plaintiff re-alleges and incorporates by reference paragraphs 1-135 of the Complaint as if fully set forth herein.

145. Plaintiff and Class Members conferred a benefit on Defendant by entrusting their PII and PHI to Defendant from which Defendant derived profits.

146. Defendant enriched themselves by saving the costs they reasonably should have expended on data security measures to secure Plaintiff and Class Members' PII and PHI. Instead of providing a reasonable level of security that would have prevented the Data Exposure, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide adequate security.

147. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

148. Defendant acquired the PII, and PHI through inequitable means in that Defendant failed to disclose the inadequate security practices, previously alleged, and failed to maintain adequate data security.

149. If Plaintiff and Class Members knew that Defendant had not secured their PII and PHI, they would not have agreed to disclosed their data to Defendant.

150. Plaintiff and Class Members have no adequate remedy at law.

151. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered—and will continue to suffer—a host of injuries, including but not limited to: (1) actual identity theft; (2) the loss of the opportunity to determine how their PII and PHI is used; (3) the compromise, publication, and/or theft of their PII and PHI; (4) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII and PHI; (5) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Exposure, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (6) the continued risk to their PII and PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI in their possession; and (7) future expenditures of time, effort, and money that will be spent trying to prevent, detect, contest, and repair the impact of Defendant's Data Exposure.

152. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members suffered—and will continue to suffer—other forms of injury and/or harm.

153. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, the benefits it received as a result of obtaining Plaintiff's and Class Members' PII and PHI.

FOURTH CAUSE OF ACTION
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

154. Plaintiff re-alleges and incorporates by reference paragraphs 1-135 of the Complaint as if fully set forth herein.

155. A relationship existed between Plaintiff, the Class Members, and Defendant, which arose from Defendant's acceptance of Plaintiff's and the Class Members' PII and PHI and Defendant's representations of its commitment to protect said PII and PHI.

156. The interests of public policy mandates that a fiduciary duty is imputed given Defendant's acceptance of Plaintiff's and the Class Members' PII and PHI and Defendant's representations of its commitment to protect said PII and PHI.

157. Defendant breached the fiduciary duty that it owed to Plaintiff and Class Members because Defendant failed to act with the utmost good faith, fairness, honesty, the highest degree of loyalty, ultimately failed to protect the PII and PHI of Plaintiff and Class Members.

158. Defendant's breach of fiduciary duty was a legal cause of damage to Plaintiff and Class Members.

159. But for Defendant's breach of fiduciary duty, the damage to Plaintiff and Class Members would not have occurred.

160. Defendant's breach of fiduciary duty contributed substantially to producing the damage to Plaintiff and Class Members.

161. As a direct and proximate result of Defendant's breach of fiduciary duty, Plaintiff and Class Members are entitled to and demand actual, consequential, nominal damages, and injunctive relief.

PRAYER FOR RELIEF

WHEREFORE Plaintiff, on behalf of himself and all others similarly situated, request the following relief:

A. An Order certifying this action as a class action and appointing Plaintiff as Class representatives and the undersigned as Class Counsel;

B. A mandatory injunction directing Defendant to adequately safeguard the PII and PHI of Plaintiff and the Class hereinafter by implementing improved security procedures and measures, including but not limited to an Order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete and purge the PII and PHI of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of Plaintiff's and Class Members' PII and PHI;

v. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring, simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;

vi. prohibiting Defendant from maintaining Plaintiff's and Class Members' PII and PHI on a cloud-based database until proper safeguards and processes are implemented;

vii. requiring Defendant to segment data by creating firewalls and access controls so that, if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

viii. requiring Defendant to conduct regular database scanning and securing checks;

ix. requiring Defendant to monitor ingress and egress of all network traffic;

x. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling

PII and PHI, as well as protecting the PII and PHI of Plaintiff's and Class Members;

xi. requiring Defendant to implement a system of tests to assess their respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xii. requiring Defendant to implement, maintain, review, and revise as necessary a threat management program to appropriately monitor Defendant's networks for internal and external threats, and assess whether monitoring tools are properly configured, tested, and updated; and

xiii. requiring Defendant to meaningfully educate all Class Members about the threats that they face because of the loss of its confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

C. A mandatory injunction requiring that Defendant provide notice to each member of the Class relating to the full nature and extent of the Data Exposure and the disclosure of PII and PHI to unauthorized persons;

D. Enjoining Defendant from further deceptive practices and making untrue statements about the Data Exposure and the stolen PII and PHI;

E. An award of damages, including actual, nominal, consequential damages, and punitive, as allowed by law in an amount to be determined;

F. An award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. An award of pre- and post-judgment interest, costs, attorneys' fees, expenses, and interest as permitted by law;

H. Granting the Plaintiff and the Class leave to amend this Complaint to conform to the evidence produced at trial;

I. For all other Orders, findings, and determinations identified and sought in this Complaint; and

J. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury for any and all issues in this action so triable as of right.

Dated: March 15, 2023

Respectfully Submitted,

/s/ H. Luke Mitcheson
H. Luke Mitcheson
MORGAN & MORGAN
1601 Trapelo Road, Suite 1601
Boston, MA 02110
Telephone: (857)-383-4905
Fascimile: (857)-383-4930
lmitcheson@forthepeople.com

JEAN S. MARTIN
(Pro Hac Vice application forthcoming)
FRANCESCA KESTER BURNE
(Pro Hac Vice application forthcoming)

MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jeanmartin@ForThePeople.com
fkester@ForThePeople.com

Counsel for Plaintiff and the Class